UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 25-CR-20021-GAYLES

UNITED STATES OF AMERICA

vs.

ERICK NTEKEREZE PRINCE,

Defendant.
_____/

FACTUAL PROFFER

The United States Attorney's Office for the Southern District of Florida and the United States Department of Justice, National Security Division (collectively, the "United States") and Erick Ntekereze Prince (hereinafter referred to as the "defendant") agree that, had this case proceeded to trial, the United States would have presented evidence proving the following beyond a reasonable doubt:

Since 2003, the government of the Democratic People's Republic of Korea ("DPRK" or "North Korea") has been under sanction by the United Nations ("UN") due to, among other things, its nuclear weapons program. Since 2016, the United States has likewise had comprehensive trade and economic sanctions against North Korea, effectively cutting North Korea off from the U.S. marketplace and financial system and restricting the ability of U.S. persons and companies from doing business with DPRK institutions. As a result, North Korea has sponsored a variety of schemes to evade these sanctions and earn money for the regime. As part of one such scheme, North Korea has dispatched thousands of highly skilled information technology ("IT") workers to obtain remote, pseudonymous employment with companies around the world. While some of these IT workers operate from cities inside North Korea, many work

in the People's Republic of China ("China") in cities near the North Korean border.

North Korean IT workers are aided in this fraud by persons residing in the United States. These U.S. facilitators receive and host laptop computers and other hardware issued by U.S. victim companies at the facilitators' residences in the United States. Using login credentials provided to them by the overseas IT workers—and unbeknownst to and without authorization from the U.S. victim companies—the U.S. facilitators then enable remote access to the laptop computers by the overseas IT workers by downloading remote desktop software (*e.g.*, AnyDesk) to the computers. The North Korean IT workers use the remote desktop software to access U.S.-based computers so that it appears to U.S. victim companies that the overseas IT workers are performing their work from U.S.-based locations. Remote desktop software applications allow a computer to remotely run another computer's desktop environment. The remote connection between devices is established and maintained through the Internet. In exchange for these and other services, many U.S. facilitators are paid a fee. Most of the money generated by this scheme, however, is funneled to the overseas IT workers and their overseas co-conspirators.

From on or about June 17, 2020 and continuing through in or around August 2024, the defendant, a U.S. citizen and resident of New York, New York, acted as a facilitator for at least three North Korean IT workers using the personas "Richard Stewart," "Pedro Alonso," "Stewart Conn," "Wesley Yang," and "Glaus Li," among others, and conspired with them to obtain their employment with U.S. companies, perform work remotely, and share in the proceeds generated by the remote IT work. At all relevant times, the defendant believed the IT workers, and Richard Stewart in particular, were Chinese nationals residing outside, and not authorized to work in, the United States. In furtherance of the scheme, the North Korean IT workers used the stolen identities of U.S. citizens to apply for and obtain remote IT work at U.S. companies. After the

North Korean IT workers obtained remote IT work, the defendant received and hosted the laptop computers issued by U.S. companies at one of the defendant's residences for the purposes of deceiving the companies into believing that the IT worker was located in the United States, as further described below.

Specifically, on July 11, 2019, the defendant contacted co-defendant Pedro Ernesto Alonso De Los Reyes ("Alonso") via Skype and informed him he was creating a new start-up company called Taggcar Incorporated ("Taggcar"). The defendant asked Alonso to join Taggcar as an iOS developer. Alonso declined, and instead, on June 17, 2020, Alonso suggested his "Chinese friend" based "in China" could help the defendant. During that conversation, Alonso admitted he had allowed this "friend" to obtain remote IT work using his name. The defendant asked Alonso to put him in touch with Alonso's "friend." Approximately two minutes later, co-defendant Jin Sung-Il ("Jin"), using the alias "Richard Stewart" and the live:richard.stewart.1202 Skype account, contacted the defendant, using the erick.nt Skype account, noting that "Pedro introduced you to me."

In May 2021, the defendant and Jin agreed to obtain remote IT work from unsuspecting United States companies through Corporation-to-Corporation ("C2C") contracts. A C2C contract is an agreement between two (or more) businesses for services, rather than an agreement between a business and an employee (or contractor) for services. As part of the scheme, the defendant agreed to use Taggcar to contract with companies to hire Jin and other overseas IT workers for remote IT work that Jin and the other overseas IT workers would ultimately complete in exchange for a 20% commission paid to the defendant. Over the course of the conspiracy, Jin introduced at least two other overseas IT workers into the scheme, including co-defendant Pak Jin-Song ("Pak").

As part of the scheme and to conceal the true identities and location of Jin, Pak, and other overseas IT workers, the defendant knowingly provided false employment certifications that contained false and stolen identity information to employers in order to obtain work for Jin, Pak, and other overseas IT workers under these false and stolen identities. As part of the scheme, the defendant also received laptops that were sent via U.S. mail or private and commercial interstate carriers to their respective residences by the U.S. companies that had hired Jin, Pak, and other overseas IT workers, while they were using false or stolen identities. The defendant then enabled Jin, Pak, and other IT overseas workers to mask their location and to perform their work through interstate and overseas wire communications by logging into those devices and installing remote desktop software without authorization. The defendant also shipped the laptops back to the victim companies via U.S. mail or private and commercial interstate carriers when victim companies terminated the employment of the overseas IT workers, including for failure to complete their work or suspicious activity.

During the course of the scheme, the defendant's North Korean co-conspirators obtained remote IT work positions using false and stolen identities from at least 64 different U.S. companies , as described above. The co-conspirators received via interstate and overseas wire transfers payment of approximately $943,069.05 for that work, including work performed by the companies identified in the indictment as Company A, Company B, Company C, and Company D. For his participation in the scheme, the defendant received more than $89,000, which was electronically transferred, via interstate and overseas wire, into a bank account he opened in the name of Taggcar.

The United States and the defendant agree that these facts are sufficient to establish the defendant's guilt as to Count 2 of the indictment.

JASON A. REDING QUIÑONES
UNITED STATES ATTORNEY

Date: 11/06/2025 By: _____
SEAN PAUL CRONIN
ASSISTANT UNITED STATES ATTORNEY

Date: 11/06/2025 By: _____
GREGORY NICOSIA
TRIAL ATTORNEY
NATIONAL SECURITY SECTION

Date: 11/6/2025 By: _____
MARISA RAYNA TANEY
ASSISTANT FEDERAL PUBLIC DEFENDER
ATTORNEY FOR DEFENDANT

Date: 11/06/2025 By: _____
ERICK NTEKEREZE PRINCE
DEFENDANT